사용자의 익명성을 제어하는 신원 위탁 방식 제안

황보성[†] · 이임영[††]

요 약

사용자가 서비스 제공자에게 인증받는 단계에서 사용자의 익명성을 제공하기 위해 키 위탁의 응용인 신원 위탁 방식을 이용한다. 신원 위탁 방식은 발행자에게 사용자의 정확한 신원을 제공하고 그에 따른 인증정보를 받는다. 사용자가 서비스 제공자에게 접근시 그의 정확한 신원을 주지 않고, 단지 이 인증정보만을 제공함으로써 사용자는 익명성을 유지한 체로 인증받을 수 있다. 하지만 사용자가 불법적 행동을 했을 경우, 서비스 제공자는 법기관에게 익명성 제거를 요청한다. 법기관은 발행자와 협력을 통해 사용자의 정확한 신원을 드러낸다. 본 논문에서는 인증 절차시 사용자의 익명성을 제공하고 유사시 법기관과 발행자와의 협력을 통해 사용자의 익명성을 제거할 수 있는 새로운 신원 위탁 방식들을 제안한다.

The Proposals of Identity Escrow Scheme to Control User's Anonymity

Bo-Sung Hwang[†] and Im-Yeong Lee[††]

ABSTRACT

We introduce the concept of a Identity Escrow Scheme, an application of key escrow ideas to solve the problem of authentication. In the Identity Escrow Scheme, the User escrows a own real identity to the Issuer and receives a Authentication Information. In authentication step, between the User to the Service Provider, the User only gives a Authentication Information to the Service Provider. Therefore, the Service Provider don't know a real identity of user's. However, when the User does unlawful actions, the Lawful Agent is called by the Service Provider, and his anonymity is revoked by cooperation of the Issuer and the Lawful Agent. We propose new Identity Escrow Schemes and analyze these.

1. 서 론

사용자들은 서비스 제공자에 접근하기 위해 자신을 증명해야 하는데 이 같은 개인식별은 사용자의 프라이버시 침해를 가져올 수 있기 때문에 사용자는 자신을 드러내지 않고 서비스를 받기를 원할 것이고 서비스 제공자는 사용자의 신원을 확인한 후 서비스를 제공하기를 원할 것이다. 두 가지 조건을 충족시켜줄 수 있는 것이 신원 위탁 방식(Identity escrow scheme)[1,2]이다. 신원 위탁 방식에서 사용자의 익명성을 제공하기 위해 사용자는 서비스 제공자에게 자신의 신원을 제공하지 않고, 발행자에 의해서 발급된 인증정보를 제공함으로써 사용자에게 익명성을 제공할 수 있다. 또한, 서비스 제공자에게는 인증정보를 통해 사용자의 신원을 알 순 없지만 정당한 사용자라는 것을 확인시킬 수 있다.

하지만, 모든 사용자에게 완전한 익명성을 제공해야 하는 것인지는 생각해 보아야할 문제이다. 어떤 사용자가 서비스 제공자에게 접근해서 불법적인 행위를 하였을 경우에는 서비스 제공자는 사용자의 익명성을 제거하고 정확한 신원을 알아야 할 것이다. 서비스 제공자는 사용자의 익명성을 제거하기 위해 사용자로부터 제공받은 인증 정보를 법기관에게 제공함으로써 그 인증 정보에 대응되는 사용자의 정확한 신원을 확보할 수 있다.

[†] 준회원, 순천향대학교 전산학과 대학원 석사과정
[††] 정회원, 순천향대학교 정보기술공학부 부교수

신원 위탁 방식은 다음과 같은 특성을 가진다.

- 사용자가 서비스 제공자에게 접근할 때 익명성을 제공한다.
- 서비스 제공자들은 유사시(사용자의 불법적인 행동) 사용자의 정확한 신원을 알 수 있다.

본 고의 2장에서는 신원 위탁 방식의 구성요소와 기본단계, 그리고 일반적 요구사항을 분석한다. 그리고 3장에서는 기존방식들에 대해 설명하고 4 장에서는 새로운 제안 방식들을 제안하고 분석한다. 마지막으로 5장에서는 결론을 맺도록 한다.

2. 신원 위탁의 일반적 개념

2.1 신원 위탁 방식의 구성요소

신원 위탁 방식은 다음과 같은 4개의 요소로 구성된다.

① 사용자 : 일반적인 사용자로써 서비스 제공자에게 익명으로 서비스를 제공받으려 한다. 이를 위해 사용자는 발행자에게 자신의 정확한 신원을 제공하고 서비스 제공자에게 익명으로 자신을 인증받을 수 있는 인증정보를 제공받는다.

② 발행자 : 익명으로 서비스 제공자에게 서비스를 제공받길 원하는 사용자의 정확한 신원을 저장하고 인증정보를 제공한다. 유사시 서비스 제공자의 요청에 의해 법기관과 협력해 사용자의 정확한 신원을 드러낸다.

③ 서비스 제공자 : 사용자의 인증정보를 확인하고 서비스를 제공한다. 만약, 사용자가 불법적 행동을 할 때에는 법기관에게 사용자의 정확한 신원을 요구한다.

④ 법기관 : 유사시 서비스 제공자의 요구를 받아 발행자와 협력해 사용자의 정확한 신원를 드러낸다.

2.2 신원 위탁 방식의 기본단계

신원 위탁 시스템은 일반적으로 다음과 같이 4단계로 나누어진다.

① 시스템 초기화 단계 : 각 참여 개체는 시스템을 초기화하기 위해 자신의 파라메터(공개키 또는 공개키 파라메터)를 공표한다.

② 신원 등록 단계 : 사용자는 자신의 정확한 신원을 발행자에게 전달하고 그에 대한 인증정보를 제공받는다.

③ 인증 단계 : 사용자는 서비스를 제공받기 위해 서비스 제공자에게 자신의 인증정보를 제공한다. 이것이 유효한 인증정보이고 사용자가 이에 따른 비밀정보를 알고 있다면 사용자는 서비스 제공자에게 익명으로 인증된다.

④ 익명성 제거 단계 : 유사시 서비스 제공자는 법기관에게 사용자가 인증시 제공한 인증정보를 제공함으로써 사용자의 익명성을 제거해 정확한 신원을 알아낸다.

2.3 신원 위탁 방식의 요구사항들

신원 위탁 방식의 일반적 요구사항을 다음과 같고 [1]에 정의되어 있다.

① 익명성을 제공하는 인증 : 사용자가 서비스 제공자에게 인증받는 단계에서 사용자의 익명성이 제공되어야 한다.

② 사용자의 익명성 제거 : 유사시 법기관의 도움에 의해 불법적 사용자에 대한 익명성을 제거할 수 있어야 한다.

③ 인증정보에 대한 비밀정보 유지 증명 : 발행자나 서비스 제공자가 사용자임을 사칭할 수 없어야 한다. 즉, 인증정보가 자기것임을 증명할 수 있는 비밀값은 사용자만이 가지고 있어야 하고 신원 위탁 시스템은 이것을 증명할 수 있어야 한다.

④ 법기관의 독립성 : 법기관은 그 특성상 오직 익명성 제거 단계에서만 신원 위탁 시스템과 연동되어야 한다.

⑤ 불법적인 익명성 제거 방지 : 사용자의 익명성 제거는 법기관의 허가내에서만 실행되어야 한다. 즉, 발행자나 서비스 제공자는 사용자의 인증정보만을 보고 사용자의 신원을 알 수 없어야 한다.

3. 기존 방식

본 장에서는 Joe Kilian, Erez Petrank가 1998년 제안한 그룹 서명을 이용한 방식과 영지식 증명(ZKIP : Zero-Knowledge Interactive Proofs)을 이용한 방식을 간단히 소개한다[1,3].

3.1 그룹 서명을 이용한 신원 위탁 방식

그룹 서명을 이용한 방식은 그룹을 감독하는 그룹 매니저에 의해 통제되는데 발행자와 법기관으로 구성된다. 그룹 매니저는 그룹에 새로운 사용자의 참여를 허락할 수 있고, 그룹의 구성자가 서명한 메시지를 증명할 수 있다(그림 1 참조).
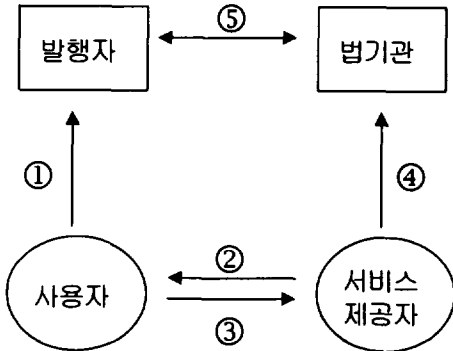
그림 1. 그룹 서명을 이용한 신원 위탁 방식

- 시스템 초기화 단계
  - 그룹 매니저(발행자, 법기관)
    RSA 파라메터 n=pq와 지수 e_1, e_2, cyclic group G=<g>를 생성하고 원소 h ∈ G를 선택한다. 그리고 ElGamal 암호 방식의 비밀키/공개키쌍(p, $y_R=h^P$)을 생성한다. 마지막으로 n, e_1, e_2, G, g, h, y_R는 공개한다.
  - 사용자
    자신의 비밀정보 x를 선택하고 다음을 계산한다.
    $y=x^{e1}$, $z=g^y$
- 신원 등록 단계

① 사용자는 발행자에게 z와 정확한 신원을 제출한다.

- 인증 단계

② 사용자가 서비스 요구자에게 서비스를 요구하면 서비스 요구자는 사용자에게 시간과 이름을 포함하는 랜덤 메시지를 준다.

③ 사용자는 x, y를 이용해 랜덤 메시지에 서명하여 서비스 제공자에게 제공한다.

- 익명성 제거 단계

④ 유사시 서비스 제공자는 법기관에게 사용자가 서명한 랜덤메시지를 준다.

⑤ 법기관과 발행자의 협력에 의해 자신의 그룹의 어떤 사용자가 서명했는지 알게 된다.

이 방식은 사용자가 서비스 제공자에게 그룹 서명을 사용함으로써 익명성을 유지시킨 채 정당한 그룹의 일원이라는 것을 증명할 수 있다. 유사시 그룹 매니저가 서명자를 확인함으로써 익명성을 제거할 수 있다. 시스템 파라메터 z가 사용자의 정확한 신원과 연결되는 값으로 발행자가 보관한다. 그리고 발행자와 법기관이 사용자의 비밀정보를 알지 못함으로 메시지를 위조할 수 없다. 하지만, 이 방식의 약점은 그룹 서명에 기반을 두고 있기 때문에 발행자와 법기관의 비독립성에 있다. 법기관은 보안상 익명성 제거시에만 호출되어야 하는데 이 방식에서는 시스템 초기화(사용자 등록시) 때도 호출된다. 또한, 발행자와 법기관의 정확한 구분이 없어 사용자가 랜덤메세지에 서명한 값을 서비스 제공자가 발행자에게 제공함으로써 법기관을 거치지 않고 불법적으로 사용자의 익명성을 제거할 수 있다.

3.2 영지식 증명을 이용한 신원 위탁 방식

Joe Kilian, Erez Petrank은 그룹 서명을 이용한 방식이 법기관의 잦은 접촉 때문에 보안상의 위험이 있다고 주장했다. 이를 해결하기 위해서는 법기관이 다른 단계에서는 관여하지 않고 오직 익명성 제거시에만 접속하는 것이 바람직하다고 주장하고 이것을 ZKIP(Zero-Knowledge Interactive Protocol)을 이용한 방법으로 설명하였다(그림 2 참조).
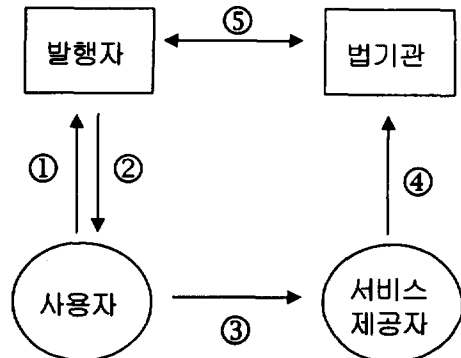
그림 2. 영지식 증명을 이용한 신원 위탁 방식

- 시스템 초기화 단계

- 발행자

RSA 파라메터 $n=p*q$, e, d를 생성하고 랜덤수 δ을 생성한다. p, q, δ는 비밀로 하고 n, e, d는 공개한다.

· 신원 등록 단계

① 사용자는 자신의 정확한 신원을 발행자에게 보낸다.

② 발행자는 사용자 신원의 low bit에 해당하는 a^e을 생성하고 $a^e-b^e=\delta$ 를 만족하는 b를 계산해 인증 정보 (a, b)를 서명해서 사용자에게 제공한다.

· 인증 단계

③ 사용자는 n에 서로소인 a_1, b_2을 선택하고 $a=a_1 \cdot a_2$ $b=b_1 \cdot b_2$을 만족하는 a_2, b_2를 선택하고 n에 서로소인 x, y를 선택한다. 영지식 증명을 이용해 다음 값들을 서비스 제공자에게 제출한다.

a_1, a_2, b_1, b_2, $(a_1)^e$, $(a_2)^e$, $(b_1)^e$, $(b_2)^e$, x, $x(a_1)^e$, $x(b_1)^e$, $x(a_1a_2)^e+y$, $x(b_1b_2)^e+y$

또한, 법기관의 공개키를 이용해 암호화한 $(a_1)^e$와 $(a_2)^e$를 제출한다. 서비스 제공자는 영지식 증명을 통해 사용자가 올바른 a, b에 대한 정보를 가지고 있는지 알 수 있다.

· 익명성 제거 단계

④ 유사시 서비스 제공자는 법기관에게 $(a_1)^e$와 $(a_2)^e$는 제출한다.

⑤ 발행자와 법기관의 협력에 의해 a에 해당하는 신원을 드러낸다.

이 방식은 인증단계에서 사용자가 서비스 제공자에게 영지식 증명을 이용해 인증정보를 가지고 있다는 것을 증명한다. 이때, 사용자의 익명성을 제거할 수 있는 추적 인자를 법기관의 공개키로 암호화하여 함께 제공한다. 유사시 서비스 제공자는 추적인자를 법기관에게 제공함으로써 사용자의 익명성을 제거할 수 있다. 이 방식은 시스템 초기화시 법기관의 접촉을 제거할 수 있다. 하지만 이 프로토콜은 발행자가 사용자의 모든 정보를 가지고 있기 때문에 사용자를 사칭할 수 있는 문제가 있다.

4. 제안방식

본 장에서는 블라인드 기술, 전자화폐 프로토콜을 기반으로 하는 새로운 신원 위탁 방식 두 가지를 제안한다.

4.1 블라인드 기술을 이용한 신원 위탁 방식 (제안 방식 1)

4.1.1 기반기술

본 논문에서는 신원 위탁 시스템의 일반적 요구사항을 만족시키기 위해 블라인드 서명[4]과 블라인드 복호[5]를 이용한다.

· 블라인드 서명

1982년 D.Chaum에 의하여 최초로 제안된 서명 방법으로 전자 현금의 불추적성을 제공하기 위해 이용된다. 최근에는 범죄 집단등에 의한 돈 세탁과 같은 전자 현금의 오용 문제를 해결하기 위하여, 필요시 전자 현금 사용자의 신원 추적이 가능한 공정한 블라인드 서명 방식이 제안되고 있다. 본 제안 방식에서는 발행자가 서명하는 메시지에 대한 내용을 추적하지 못하게 하기 위해 블라인드 서명을 이용한다. 블라인드 서명의 일반적 방식은 다음과 같다.
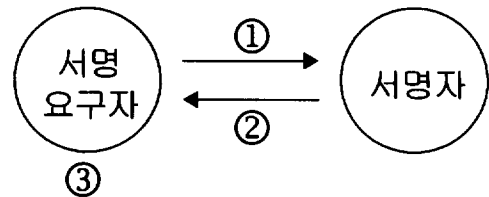
그림 3. 블라인드 서명

① 서명 요구자는 메시지에 블라인드 서명을 받기 위해 $X = Mr^e \bmod n$ 생성을 생성하고 이를 서명자에게 전달한다.

(M : 서명 받고자 하는 메시지, r : 랜덤값, e : 서명자의 공개키)

② 서명자는 X에 자신의 비밀키로 다음과 같이 서명하고 서명 요청자에게 전달한다. 서명자는 M에 대한 내용을 알지 못한 체 서명한다.

$$X^d = (Mr^e)^d = M^d r$$

③ 서명 요청자는 다음과 같이 서명자로부터 서명된 메시지를 얻는다.

$$M^d r / r = M^d$$

· 블라인드 복호

블라인드 복호의 기본 개념은 복호자는 자신이 복호한 메시지의 내용을 모른 체 자신의 비밀키를 이용

해 메시지를 복호해 주는 것이고, 복호 요구자는 복호자의 비밀키를 모른 체 메시지를 알 수 있는 방식이다. 본 제안 방식에서는 사용자가 서비스 제공자에게 인증정보에 해당하는 메시지를 구성하는 비밀정보를 알고 있다는 것을 증명하기 위해 이용한다. 보통 블라인드 복호는 3명의 구성요소로 구성되며 본 제안방식 또한 그렇다. 간편한 이해를 위해 여기서는 2명이 참가하는 일반적인 블라인드 복호 프로토콜을 설명한다.
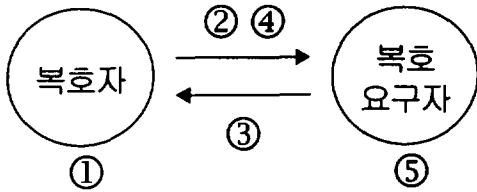
그림 4. 블라인드 복호

① 복호자는 자신의 키쌍 $P_u = g^s \bmod p$ 생성(s:비밀키, P_u:공개키)을 생성한다.

② 메세지를 생성 후 블라인드 복호 프로토콜을 위해 C = (C_1, C_2)을 생성하고 C를 복호요구자에게 전달한다.

$C_1 = g^r \bmod p$, $C_2 = P_u^r M \bmod p$ (M : 메세지, r : 랜덤수)

③ 복호 요구자는 블라인드 복호를 위해 랜덤수 a를 생성하고 $X = C_1^a$를 계산한다. 그리고 X를 복호자에게 전달한다.

④ 복호자는 자신의 비밀키로 $Y = X^s \bmod p$을 계산 후 Y를 복호 요구자에게 전달한다.

⑤ 복호 요구자는 $(Y)^{-a} = (C_1^{as})^{-a}$을 계산하고 다음과 같이 메세지를 추출한다.

$$C_2 / C_1^s = M$$

4.1.2 제안 프로토콜

- 시스템 초기화 단계
- 발행자, 법기관
  자신의 공개키와 공개키에 해당하는 파라메터를 공개한다.
- 신원 등록 단계(그림 5 참조)

① 사용자는 랜덤값 r를 생성하고 이를 법기관에게 전송한다.
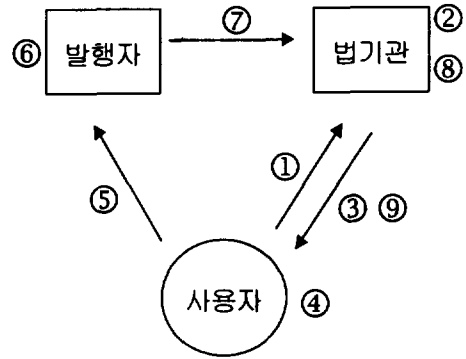
그림 5. 신원 등록 단계
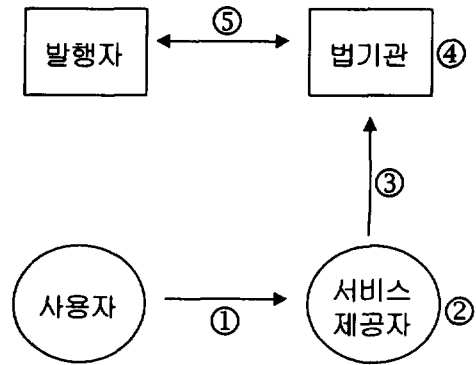
그림 6. 인증 및 익명성 제거 단계

② 법기관은 일련번호(DN)와 승인정보를 생성한다. 법기관이 가지는 있는 정보는 사용자에 해당하는 일련번호(DN)와 r값이다.

③ 법기관은 다음을 생성해 사용자에게 전송한다.

$M = S_E[\, K_{KP_E}(DN) \,\|\, 승인정보 \,\|\, r],\ DN$

(S_E : 법기관의 서명, $K_{KP_E}(DN)$: 법기관의 공개키로 암호화된 DN)

④ 사용자는 발행자에게 메시지를 숨긴 체 서명받기 위해 다음과 같은 X를 생성하고 블라인드 복호 파라메터를 생성한다.(그림 3,4 참조)

$$X = Mr^e \bmod n,\ C = (C_1, C_2)$$

(e : 발행자의 공개키, X : 블라인드 서명 파라메터, C : 블라인드 복호 파라메터)

⑤ 사용자는 발행자에게 DN, X, 신원정보, C_2를 제공한다.

⑥ 발행자는 X를 다음과 같이 블라인드 서명한다.

$$X^d = (Mr^e)^d = M^d r$$

발행자는 각 사용자에 해당하는 DN과 신원정보

를 가진다.

⑦ 발행자는 법기관에게 DN, $M^d r$, C_2를 제공한다.

⑧ 법기관은 $M^d r$에서 r을 제거 후 M^d의 내용을 확인하다. 확인하는 내용은 r과 DN이다.

⑨ 마지막으로 법기관은 다음을 사용자에게 전송하고 이 값은 사용자가 서비스 제공자에게 인증시 이용되는 인증정보이다.

$$인증정보 = C_2M^d,\ S_E(H(C_2M^d))$$

• 인증 단계(그림 6 참조)

① 사용자는 서비스 제공자에게 접속시 다음을 서비스 제공자의 공개키로 암호화해서 전달한다.

$$C_1,\ 인증정보$$

② 서비스 제공자는 블라인드 복호 과정을 거쳐 M^d를 획득하고 발행자와 법기관의 서명을 확인한다. 그리고 승인정보를 검증하여 사용자를 인증한다.

• 익명성 제거 단계(그림 6 참조)

③ 사용자가 불법적 행동을 하였을 경우, 서비스 제공자는 사용자의 익명성을 제거하기 위해 법기관에게 M^d를 제출한다.

④ 법기관는 M^d에서 DN을 추출해낸다.

⑤ 발행자와 합의해서 사용자의 신원을 드러낸다.

4.1.3 제안 방식 분석

제안 방식은 블라인드 기술을 이용해 신원 위탁 시스템의 요구사항을 만족시키고자 하였다.

- 블라인드 서명

사용자가 서명하는 메시지에 대한 내용을 알지 못하게 하기 위해 이용된다. 이 방법을 이용해 발행자와 서비스 제공자와의 공모에 의해 사용자의 신원이 드러나는 것을 방지할 수 있다. 즉, 인증단계에서 발행자가 사용자로부터 서비스 제공자에게 제출되는 인증정보만을 보고 사용자의 익명성을 제거하는 것을 방지할 수 있다는 것이다.

- 블라인드 복호

사용자가 인증정보에 대한 비밀정보를 가지고 있는가에 대한 인증 단계에 이용된다. 즉, 서비스 제공자에게 인증정보안의 블라이드 복호 파라메터(C_2)를 제거하고 메시지를 확인시켜 줄 수 있는 구성요소는 비밀키(s)를 가지고 있는 사용자만이 가능하다. 그러므로, 사용자의 비밀키를 모르는 다른 구성요소들은 사용자임을 사칭할 수 없다.

또한, 신원 등록 단계에서 사용자의 정확한 신원은 발행자가 가지고 있고 이 정확한 신원과 연결되는 정보(DN : 인증정보에 포함된 일련번호)는 법기관만이 접근할 수 있다. 따라서 발행자와 법기관이 협동해야만 사용자의 신원을 알아 낼 수 있고 혼자서는 사용자의 신원을 알 수 없다. 하지만 이 방법은 시스템 초기화시 법기관과의 접촉이 요구된다.

4.2 전자 화폐 프로토콜을 이용한 신원 위탁 방식 (제안 방식 2)

4.2.1 기반 기술

• 전자화폐 프로토콜

초기의 전자화폐에서는 사용자의 프라이버시를 제공하기 위해 동전이나 사용자에 익명성을 제공하였다. 하지만 이러한 익명성은 사용자의 범법적 행동을 용이하게 할 수 있기 때문에 제한적으로 사용자나 익명성을 제거할 수 있는 방법들이 소개되고 있다 [6]. 익명성 제어가 가능한 전자화폐 프로토콜을 이용해 신원 위탁 방식의 요구사항을 만족시킬 수 있다. 따라서 본 논문에서는 S.Brands의 논문[7]을 기반으로 법기관의 독립성뿐만 아니라, 신원 위탁 방식에서 다른 구성원이 사용자의 신원을 사칭할 수 없는 안전성을 향상시킨 새로운 방식을 제안한다(그림 7 참조).
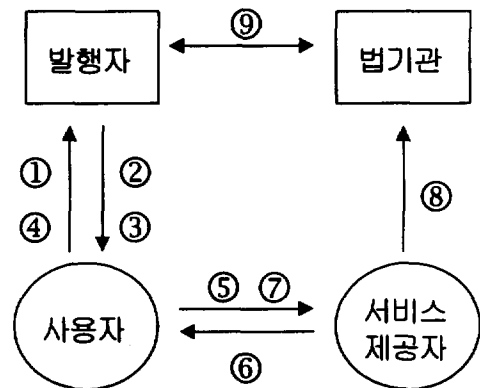
그림 7. 전자화폐 프로토콜을 이용한 신원 위탁 방식

4.2.2 제안 프로토콜

• 시스템 초기화 단계

- 발행자

$g_i \in G_q$을 만족하는 원시근 g, g_1, g_2와 해수함수 H를 공개한다.

· 신원 등록 단계

① 사용자는 랜덤값 p를 생성하고 $I = g_1^p$ 을 계산하여 발행자에게 I와 정확한 신원을 전송한다. p는 사용자의 비밀정보이다.

② 발행자는 사용자의 정확한 신원과 I를 저장하고 발행자의 비밀키 x로 $z = (Ig_2)^x$를 계산한다. 그리고 법기관의 공개키로 z를 암호화하고 발행자의 비밀키로 서명을 붙여 z와 $Sign_{issuer}[E_{KP_E}(z)]$를 사용자에게 전송한다. g_1^x과 g_2^x을 자신의 공개키의 일부로서 공개하고 x는 비밀로 보관한다.

③ 발행자는 랜덤값 w을 생성하고 사용자에게 $a = g^w$와 $b = (Ig_2)^w$를 전송한다.

④ 사용자는 랜덤값 s, x_1, x_2, l, n을 생성하고 $A = (Ig_2)^s$, $B = g_1^{x_1} g_2^{x_2}$, $z' = z^s$, $a' = a^l g^n$, $b' = b^{sl} A^n$를 계산한다. 사용자는 그때 challenge 값 $c' = H$(A, B, z', a', b')을 계산하고 c'를 은닉시키기 위해 challenge c = c'/l mod q를 발행자에게 전송한다. 발행자는 r=cx+w mod q를 계산해 사용자에게 되돌린다. 사용자는 $g^r = h^c a$ 와 $(Ig_2)^r = Z^c b$ 을 만족한다면 인증정보가 제대로 구성된 것으로 판단한다. 이러한 과정을 거쳐 사용자는 인증정보에 해당하는 sign(A, B)를 확인 받게 된다. sign(A,B)는 다음을 만족한다.

$$g^r = h^{H(A,\ B,\ z,\ a,\ b)} a$$
$$A^r = z^{H(A,\ B,\ z,\ a,\ b)} b$$

· 인증 단계

⑤ 사용자는 서비스 제공자에게 A, B, sign(A, B)와 $Sign_{issuer}[E_{KP_E}(z)]$를 제출한다.

⑥ 서비스 제공자는 challenge 값 d=H(A, B, date/time)을 계산하고 d를 사용자에게 전송한다.

⑦ 사용자는 response 값 $r_1 = d(ps) + x_1 \bmod q$와 $r_2 = ds + x_2$을 계산하고, 그것들을 서비스 제공자에게 전송하면 $g_1^{r_1} g_2^{r_2} = A^d B$과 sign(A, B)값이 만족하는지 검사 후 사용자를 인증한다.

· 익명성 제거 단계

⑧⑨ 유사시 서비스 제공자는 법기관에게 Sign[$E_{KP_E}(z)$]을 제출하고 발행자와의 협력에 의해서 사용자의 신원을 드러낸다.

4.2.3 제안 방식 분석

제안 방식은 법기관의 독립성을 유지(신원 위탁 단계에 참여하지 않는다.)하고 사용자의 신원 사칭을 방지하고 있다. 신원 등록 단계에서 사용자는 정확한 신원과 그 신원을 알아낼 수 있는 I를 발행자에게 제공하고, 발행자는 사용자에게 인증정보를 제공받을 수 있는 z를 사용자에게 되돌린다. 사용자는 제공받은 z를 이용해 발행자와 협력하여 인증 단계에서 사용될 인증정보 A, B를 만든다. 인증 단계에서 사용자는 서비스 제공자에게 A, B, sign(A, B), $Sign_{issuer}[E_{KP_E}(z)]$를 주고 사용자가 A, B를 구성하는 비밀정보를 가지는 있는지 확인하기 위해 challenge 값을 생성하고, 사용자는 그 값에 해당하는 비밀정보를 response 값으로 전송함으로써 사용자를 인증한다.

발행자와 서비스 제공자는 식별자의 비밀정보를 알지 못하기 때문에 사용자를 사칭할 수 없고 시스템 초기화 단계에서는 법기관의 참여가 없고 오직 서비스 제공자의 익명성 제거 요구가 있을 경우에만 참여하기 때문에 법기관은 독립적이다.

4.3 신원 위탁 방식 비교

지금까지 두 가지 기존 방식과 두 가지의 새로운 신원 위탁 방식들을 살펴보았고 [표 1]은 이 네 가지 방식들을 비교한 것이다.

그룹 서명 방식은 사용자의 익명성을 제공하기 위해 그룹 서명 기술을 이용한 것으로 법기관이 신원 등록 단계에서 참여하는 단점을 가진다. 영지식 증명 방식은 그룹 방식의 단점을 해결하기 위해 영지식 증명 기술을 이용하였으나 사용자의 비밀정보를 발행자가 알고 있다는 단점을 가진다. 제안방식 1은 블라인드 기술을 이용해 사용자의 익명성을 제공하였고, 이 방식 또한 그룹 서명 방식과 같이 법기관이 신원 등록 단계에 참여한다는 단점을 가진다. 제안 방식 2는 요구사항들을 만족시키기 위해 전자화폐 프로토콜을 이용하였다.

5. 결 론

지금까지 기존의 신원 위탁 방식을 소개하고 여러 가지 기능이 향상된 새로운 신원 위탁 방식 두 가지를 제안하였다. 사용자가 네트워크 상에서 서비스 제

표 1. 신원 위탁 방식들 비교

	익명성을 제공하는 인증	사용자의 익명성 제거	사용자의 비밀정보 유지 증명	법기관의 독립성	불법적인 익명성 제거 방지
그룹 서명을 이용한 방식	○	○	○	×	○
영지식 증명을 이용한 방식	○	○	×	○	×
제안방식 1	○	○	○	×	○
제안방식 2	○	○	○	○	○

공자에게 접속할 때 자신의 신원을 정확히 알려주느냐, 그렇지 않느냐의 문제는 사용자와 서비스 제공자에게는 아주 민감한 문제이다. 사용자는 자신의 신원을 숨긴 채 서비스 받기를 원할 것이고, 서비스 제공자는 사용자의 정확한 신원확인 후 서비스를 제공하기를 원할 것이다. 이렇게 상충되는 의견은 키 위탁[8-10]을 변형한 신원 위탁 방식을 사용함으로써 사용자와 서비스 제공자 모두에게 소기의 목적을 달성할 수 있을 것이다. 향후 연구분야로 기존 방식들과 제안 방식들에 대한 구현이 필요할 것이고 이에 대해 발생하는 문제점 및 효율성 분석이 필요할 것이다.

참 고 문 헌

[1] Joe Kilian and Erez Petrank, "Identity Escrow", Advances in Crytology-CRYPTO '98, pp. 169-184, 1998.
[2] Joe Kilian and Erez Petrank, "Identity Escrow", Theory of Cryptography Library, ftp://theory.lcs.mit.edu/pub/tcrypto1/97-11.ps, 1997.
[3] Camenisch, "Efficient and generalized group signatures", Advances in Cryptology-EUTOCRYPT '97, pp. 465-479, 1997.
[4] M. Stadler, "Fair blind signatures", In Proc. Eurocrypt 95, 1995, LNCS 921, pp. 209-219.
[5] Kouichi Sakurai and Yoshinori Yamane, "Key Escrow system of Protecting User's Privacy by Blind Decoding", pp. 147-157, 1998.
[6] 오형근, 이임영, "익명성 제어 기능을 가지는 전자화폐 프로토콜에 관한 연구", '98통신정보보호학회 종합학술 발표회(CISC'98), pp. 109-121, 1999.
[7] S.Brands, "Untraceable Off-line Cash in Wallets with Observers", Processdings of Crypto '93, pp. 302-318.
[8] Silvio Micali, "Fair Cryptosystems", Advances in Cryptology-CRYPTO '92, pp. 113-138, 1992.
[9] "Requriements for Key Recovery Prodeucts", NIST, http://csrc.nist.gov, 1998.
[10] Approval of FIPS 185 "Escrowed Encryption Standard(EES)", http://www.epic.org, 1994.

황 보 성

1999년 2월 순천향대학교 전산학과 졸업
1999년 3월~현재 순천향대학교 전산학과 대학원 석사과정
관심분야 : 암호 이론, 컴퓨터 보안

이 임 영

1981년 8월 홍익대학교 전자공학과 졸업
1986년 3월 오사카대학 통신공학과 석사
1989년 3월 오사카대학 통신공학과 박사
1989년 1월~1994년 2월 한국전자통신연구원 선임연구원
1994년 3월~현재 순천향대학교 정보기술공학부 부교수
관심분야 : 암호이론, 정보이론, 컴퓨터 보안